Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 5 octobre 2018

Présents: Delphine Boucher, Sylvain Duquesne, Pierre Loidreau, Elisa Lorenzo-Garcia, Blodwen Meynier (M1 l'an dernier), Christophe Ritzenthaler, Andy Russon (M2 l'an dernier).
Absents excusés: Patrick Derbez, Eric Gousset

Bilan du second semestre de M1

- « Complexité»
  BM : assez bien apprécié. Mise en route un peu difficile car nouveau. Nouveau volume horaire bien adapté.
- « Codes correcteurs (COCO)»
  BM : super organisation du cours et prof très à l'écoute. TP trop longs et pas très au clair de ce qui est évalué dans les TP. Content d'avoir une note de TP et un retour sur le travail réalisé. Un retour comme quoi le contenu ne serait pas assez récent sur la partie crypto
  SD/DB : ce n'est pas grave si c'est long à terminer. C'est clair qu'on attend du travail et de l'investissement en dehors des cours.
  DB: Pourquoi pas ne pas noter les TP (mais c'est ca qui remonte les moyennes). Ou alors des questions de programmation sur papier lors des contrôles continus.
  CR : Au pire, une notation rapide est possible. Les TP ca sert surtout à comprendre ce qui se passe dans le cours, ce n'est pas forcément le but de vérifier que le code est propre et optimisé.
  Tous : ce serait bien de faire un cours de M2 en codes pour la crypto à l'avenir. A réfléchir pour l'an prochain.
- « Théorie des nombres (THNO) »
  BM :Globalement très bien mais au vidéoprojecteur. Illisible et lit les transparents. Quelques doublons avec ALGB. TD à faire à la maison mais sans corrections ensuite. Enoncés de TD parfois donnés trop tardivement.
  SD : le module disparaît, ou plutôt est intégré à ALGB en échange de la théorie de Galois.
- « Cryptographie (CRYP)»
  BM : Rien à dire sur le cours. Gros décalage en TD, pas de lien avec le cours, peu voire pas d'aide en TP. Pas clair sur l'évaluation en CC. Les passages au tableau sont appréciables mais du coup, il n'y pas de correction type.
  SD : L'intervenant de TD/TP change cette année.
- « Projet tutoré»
  BM : Pas tutoré, impression d'être lâchés dans le vide. Par contre c'est bien d'avoir du temps pour le faire après les cours.
  DB: En TER, il y a un prof référent et on les voit une fois par semaine. Ils travaillent sur un article.
  CR/EL : une fois par semaine au prix où c'est payé, ce n'est pas raisonnable.
  SD : C'est un problème récurrent. Les enseignants sont disponibles mais les étudiants ne viennent pas vers eux. L'aspect autonomie est fondamental à garder pour se préparer aux stages et à l'insertion professionnelle. Ceci dit, c'est vrai que cette année, c'était particulièrement mal organisé, en particulier sur les enseignants affectés aux sujets. On organisera mieux cette année.
- « Anglais»
  BM : Tout s'est très bien passé. Encourage à prendre la parole. Super
  Tous : Enfin un retour positif. Le niveau global a très clairement augmenté, au moins en compréhension
- Bilan global :
  BM : Algèbre de très haut niveau mais on le savait. Prévenus trop tard pour le DSA en particulier pour ceux qui travaillent l'été.
  SD : On fera plus tôt dorénavant. 21 étudiants ont suivi le parcours, 15 ont validé l'année, 1 redouble.

Bilan du second semestre de M2

AR : Globalement très peu de retours (étudiants pris leur emploi ou leur recherche d'emploi)

- « Sécurité des implémentations (SIMP)»
  AR : très bon cours et les TP sont très bien et permettent de bien voir les attaques. Seul le premier TP était noté et c'était très bien. Salle de TP pas adaptée (trop petite).
  SD : On ne peut malheureusement pas faire grand-chose pour la salle car elles sont globalement surchargées. Il y a des projets de nouvelles salles mais en attente de financements
- « Courbes elliptiques en Cryptographie (CEC)»
  AR :TB et intéressant d'utiliser magma en TP car ca change et c'est bien de s'habituer à d'autres langages.
- « Théorie algorithmique des nombres »
  AR : Très bien, mais certains algos sont déjà vus en M1. Ce serait mieux de passer moins de temps dessus.
- **AR** : Intervention sur le droit du numérique intéressante et utile. Ne permet bien sûr pas d'approfondir mais au moins d'être conscient des problématiques.
- Globalement
  AR : Organisation de la session 2 de Java très mauvaise (étudiants prévenus au dernier moment et par hasard)
  SD : session 2 très mal organisée globalement, à la fois à cause de la scolarité (typiquement pour Java) et à cause d'une mauvaise compréhension (ou explication) des principes régissant la session 2 à Rennes 1. Ca a été rattrapé en jury (en particulier en reprenant les notes de session 1 des étudiants qui ne sont pas venus en session 2 et auraient du avoir 0.

Bilan des stages de M2

SD : Encore une fois, les stages se sont globalement très bien passés. Certains ont toutefois eu des difficultés à trouver un stage, en particulier les étrangers.
Les 16 étudiants présents ont validé l'année, 1 a abandonné en cours d'année et 3 étaient inscrits mais ne sont jamais venus. A ce jour 10 de ces 16 étudiants ont trouvé un emploi ou une thèse et 2 sont en très bonne voie (finalisation des démarches). Les 4 autres n'ont pas encore trouvé d'emploi.

Point sur la rentrée

La sélection se fait en M1, une centaine de candidatures a été reçue dont 22 de Rennes, 6 du périmètre CHL, 32 d'ailleurs en France, 35 de l'étranger dont 33 via Campus France. C'est moins que l'an dernier au global mais la baisse vient uniquement de Campus France qui opère une présélection à partir de cette année pour éviter que des étudiants acceptés dans des diplômes se voient finalement refuser le visa (ce qui n'empêche pas un étudiant d'être dans ce cas cette année).

33 ont été acceptés (+4 sur Campus France) et finalement seulement 14 inscrits (+1 Campus France mais qui n'a toujours pas obtenu son visa). C'est du à des désistements de dernière minute, voire même pas explicités ce qui a empêché d'avancer sur la liste complémentaire une fois la rentrée passée. Plusieurs étudiants sont intéressés par le double diplôme.
Une étudiante acceptée et qui avait préféré aller à Bordeaux souhaiterait revenir. Malgré les difficultés due à une arrivée si tardive, cela reste possible.

En M2, il y avait 17 candidatures extérieures. 3 ont été acceptées et 2 sont venues. Il y a finalement 15 étudiants en cours dont 2 inscrits dans le parcours recherche. Il faut rajouter à cela 5 étudiants du double diplôme actuellement en Allemagne, un étudiant en année de Césure au Japon et un étudiant de la promo 2014 qui n'avait pas validé son stage. Au total, il y a donc 22 inscrits en M2.

L'emploi du temps est très chargé en ce début d'année en M2. Ca peut préfigurer ce qu'on attendra des étudiants dans le monde professionnel mais c'est d'autant plus difficile qu'il faut jongler entre des thématiques très variées et souvent à coté d'étudiants spécialistes des sujets abordés. Il n'y a malheureusement pas grand-chose à faire étant données les contraintes. Le cours de courbes elliptiques pour la cryptographie est déjà reporté à des jours meilleurs.